DECLARATION

I, NOBUAKI KATO, a Japanese Patent Attorney registered No. 8517, of Okabe International Patent Office at No. 602, Fuji Bldg., 2-3, Marunouchi 3-chome, Chiyoda-ku, Tokyo, Japan, hereby declare that I have a thorough knowledge of Japanese and English languages, and that the attached pages contain a correct translation into English of the priority documents of Japanese Patent Application No. 11-325559 file on November 16, 1999 in the name of CANON KABUSHIKI KAISHA.

I further declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made, are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

Signed this 4 th day of August, 2006

NOBUAKI KATO

PATENT OFFICE
JAPANESE GOVERNMENT

This is to certify that the annexed is a true copy of the following application as filed with this office.

Date of Application: November 16, 1999

Application Number: Japanese Patent Application No. 11-325559

Applicant(s): CANON KABUSHIKI KAISHA

December 8, 2000

Commissioner,
Patent Office OIKAWA KOZO

(Seal)
Certificate No. 2000-3102649

11-325559

[Name of the Document] Patent Application

[Reference No.] 4038149

[Date] November 16, 2001
[Addressed to] Commissioner of the Patent Office

[International Classification] H04N 1/00 107

H04L 9/00 601

[Title of the Invention] COMMUNICATION APPARATUS, METHOD AND MEMORY MEDIUM THEREFOR

[Number of the Claims] 30

[Inventor]

[Domicile or Residence] c/o Canon Kabushiki Kaisha
30-2, 3-chome, Shimomaruko,
Ohta-ku, Tokyo

[Name] EIICHI SATO

[Applicant]

[Identification No.] 000001007

[Name] CANON KABUSHIKI KAISHA

FUJIO MITARAI

[Telephone Number] 03-3758-2111

[Attorney]

[Identification No.] 100090538
[Domicile or Residence] c/o Canon Kabushiki Kaisha

30-2, 3-chome, Shimomaruko,

Ohta-ku, Tokyo

[Patent Attorney]

[Name] KEIZO NISHIYAMA

[Telephone Number] 03-3758-2111

[Elected Attorney]

[Identification No.] 100096965

[Domicile or Residence] c/o Canon Kabushiki Kaisha
30-2, 3-chome, Shimomaruko,
Ohta-ku, Tokyo

[Name] YUICHI UCHIO

[Telephone Number] 03-3758-2111

[Elected Attorney]

[Identification No.] 100110009

[Domicile or Residence] c/o Canon Kabushiki Kaisha
30-2, 3-chome, Shimomaruko,
Ohta-ku, Tokyo

[Name] YASUSHI AOKI

[Telephone Number] 03-3758-2111

[Elected Attorney]

[Identification No.] 100069877

[Domicile or Residence] c/o Canon Kabushiki Kaisha
30-2, 3-chome, Shimomaruko,
Ohta-ku, Tokyo

[Name] YOSHIKAZU MARUSHIMA

[Telephone Number] 03-3758-2111

[Indication of Official Fee]

[Prepayment Ledger No.] 011224

[Amount] ¥21000

[List of Filed Materials]

[Material] Specification 1

[Material] Drawings 1

[Material] Abstract 1

[General Power of Attorney] 9908388

[Proof requirement] necessary

Applicant's Information

Identification No. [000001007]

1. Date of Change: August 30, 1990

(Reason of Change) New Registration

Address: 3-30-2, Shimomaruko, Ohta-ku, Tokyo

Name: CANON KABUSHIKI KAISHA

CFO14924

11-325559

[Name of the Document] Specification

[Title of the Invention] Communication Apparatus, Method and Memory Medium Therefor

[Claim(s)]

[Claim 1] A communication apparatus for transferring data received from a first network to a second network, the apparatus comprising:

first discrimination means for discriminating the destination of said received data;

second discrimination means for discriminating the secrecy level of said received data; and

control means for executing the transfer of said received data, according to a method based on the result of discrimination by said first and second discrimination means.

[Claim 2] The communication apparatus according to claim 1, wherein said control means selectively executes the encryption of said received data.

[Claim 3] The communication apparatus according to claim 1, wherein said control means selectively transfers to said destination by e-mail.

[Claim 4] The communication apparatus according to any one of claims 1 to 3, wherein said control means selectively uploads said received data to a predetermined server computer on said second network.

[Claim 5] The communication apparatus according to any one of claims 1 to 4, wherein said second discrimination means discriminates whether said received data are confidential data.

[Claim 6] A communication apparatus comprising:

receiving means for receiving data from a first network;

storage means for storing said data in a predetermined memory box;

transfer means for transferring said data to a destination on a second network;

management means for managing destination information on said second network; and

discrimination means for discriminating whether said management means holds an encryption key corresponding to said destination,

wherein when said discrimination is affirmative, after encrypting said data by said encryption key, said transfer means is executed, and

when said discrimination is negative, said storage means is executed to said data.

[Claim 7] The communication apparatus according to claim 6, wherein when the discrimination by said discrimination means is negative, a message indicating that said data are stored in the memory box is transmitted to said destination.

[Claim 8] The communication apparatus according

to claim 6 or 7, wherein said encryption key is a public key acquired from said destination.

[Claim 9] The communication apparatus according to any one of claims 6 to 9 further comprising secrecy level discrimination means for discriminating the secrecy level of said data, wherein any data a secrecy level of which is low are transferred to said destination without encrypting regardless of the result of said discrimination means.

[Claim 10] The communication apparatus according to claim 9, wherein said secrecy level discrimination means discriminates whether said data are confidential data.

[Claim 11] The communication apparatus according to any one of claims 6 to 8 further comprising security discrimination means for discriminating security of the transfer path to said destination,

wherein when the destination is judged secure, the data is transferred without encrypting regardless of the result of said discrimination means.

[Claim 12] The communication apparatus according to claim 6 or 7 further comprising detection means for detecting that the discrimination of said discrimination means becomes affirmative after executing said storage means,

wherein when said detection means detects the affirmative discrimination, said transfer means

transfers the data in said memory box.

[Claim 13] The communication apparatus according to any one of claims 1 to 12, wherein said first network is the public network and said second network is LAN.

[Claim 14] The communication apparatus according to any one of claims 1 to 12, wherein said first network is the circuit switching network and the transfer path of said second network contains the internet.

[Claim 15] A communication method for transferring data received from a first network to a second network, the method comprising:

a first discrimination step of discriminating the destination of said received data;

a second discrimination step of discriminating the secrecy level of said received data; and

a control step of executing the transfer of said received data, according to a method based on the result of discrimination by said first and second discrimination steps.

[Claim 16] The communication method according to claim 15, wherein said control step selectively executes the encryption of said received data.

[Claim 17] The communication method according to claim 15, wherein said control step selectively transfers to said destination by e-mail.

[Claim 18] The communication method according to any one of claims 15 to 17, wherein said control step selectively uploads said received data to a predetermined server computer on said second network.

[Claim 19] The communication method according to any one of claims 15 to 18, wherein said second discrimination step discriminates whether said received data are confidential data.

[Claim 20] A communication method comprising:

a receiving step of receiving data from a first network;

a storage step of storing said data in a predetermined memory box;

a transfer step of transferring said data to a destination on a second network;

a management step of managing destination information on said second network; and

a discrimination step of discriminating whether said management means holds an encryption key corresponding to said destination,

wherein when said discrimination is affirmative, after encrypting said data by said encryption key, said transfer step is executed, and

when said discrimination is negative, said storage step is executed to said data.

[Claim 21] The communication method according to claim 20, wherein when the discrimination by said

discrimination step is negative, a message indicating that said data are stored in the memory box is transmitted to said destination.

[Claim 22] The communication method according to claim 19 or 20, wherein said encryption key is a public key acquired from said destination.

[Claim 23] The communication method according to any one of claims 20 to 22 further comprising a secrecy level discrimination step of discriminating the secrecy level of said data, wherein any data a secrecy level of which is low are transferred to said destination without encrypting regardless of the result of said discrimination step.

[Claim 24] The communication method according to claim 23, wherein said secrecy level discrimination step discriminates whether said data are confidential data.

[Claim 25] The communication method according to any one of claims 20 to 22 further comprising a security discrimination step of discriminating security of the transfer path to said destination,

wherein when the destination is judged secure, the data is transferred without encrypting regardless of the result of said discrimination means.

[Claim 26] The communication apparatus according to claim 20 or 21 further comprising detection means for detecting that the discrimination of said

discrimination means becomes affirmative after executing said storage means,

wherein when said detection means detects the affirmative discrimination, said transfer means transfers the data in said memory box.

[Claim 27] The communication method according to any one of claims 14 to 24, wherein said first network is the public network and said second network is LAN.

[Claim 28] The communication method according to any one of claims 14 to 24, wherein said first network is the circuit switching network and the transfer path of said second network contains the internet.

[Claim 29] A computer readable memory medium storing a program of a communication method for transferring data received from a first network to a second network, the program comprising:

a first discrimination step of discriminating the destination of said received data;

a second discrimination step of discriminating the secrecy level of said received data; and

a control step of executing the transfer of said received data, according to a method based on the result of discrimination by said first and second discrimination steps.

[Claim 30] A computer readable memory medium comprising:

a receiving step of receiving data from a first

network;

a storage step of storing said data in a predetermined memory box;

a transfer step of transferring said data to a destination on a second network;

a management step of managing destination information on said second network; and

a discrimination step of discriminating whether said management means holds an encryption key corresponding to said destination, wherein

when said discrimination is affirmative, after encrypting said data by said encryption key, said transfer step is executed, and

when said discrimination is negative, said storage step is executed to said data.

[Detailed Description of the Invention]

[0001]

[Field of the Invention]

The present invention relates to a communication apparatus suitable for transferring the received secret data.

[0002]

[Prior Art]

Owing to the recent remarkable popularization of the internet, the facsimile device which has executed communication only through the public network is now becoming to be connected to a computer network such as

a LAN (local area network).

[0003]

Fig. 9 illustrates an example of using a facsimile device adaptable to multi lines connectable to the public network and the LAN. In Fig. 9, reference number 901 denotes a facsimile device adaptable to multi lines; 902, a facsimile device adaptable only to the public network; 903, a server for storing image data; and 904, a client computer which can exchange information with the server. Upon receiving image data from another facsimile device 902 through the public network 202, the facsimile device 901 transfers such image data to a server computer 903 through the LAN 203.

[0004]

The user acquires the image data by accessing to the server computer 903. The acquired image data are displayed and viewed on a CRT by a predetermined viewer software.

[0005]

In the facsimile communication, there is known a confidential function. In such function, the facsimile apparatus does not immediately print the image received under the designation of a confidential transmission but stores the image in a memory, and prints such image from the memory in response to the input of a predetermined password. Thus the image can be viewed only by the user who knows the confidential password.

[0006]

[Problem to be Solved by the Invention]

However, as the conventional facsimile device described above is not provided with a configuration for transferring the confidential image, the intended recipient user of the confidential image has to go to the location of such facsimile device and to have the confidential image to be printed by the entry of the password.

[0007]

In consideration of the foregoing, an object of the present invention is to provide a communication apparatus capable of transferring the received confidential image to a predetermined destination while maintaining its confidential character, and a method and a memory medium therefor.

[0008]

[Means for Solving the Problem]

In order to achieve the above object, a present invention is a communication apparatus for transferring data received from a first network to a second network, the apparatus comprising first discrimination means for discriminating the destination of the received data; second discrimination means for discriminating the secrecy level of the received data; and control means for executing the transfer of the received data, according to a method based on the result of

discrimination by the first and second discrimination means.

[0009]

Preferably, the control means selectively executes the encryption of the received data on the basis of the result of discrimination by the first and second discrimination means.

[0010]

Preferably, the control means selectively transfers to said destination by e-mail on the basis of the result of discrimination by the first and second discrimination means.

[0011]

Preferably, the control means selectively uploads the received data to a predetermined server computer on the second network.

[0012]

Preferably, the second discrimination means discriminates whether the received data are confidential data.

[0013]

Another present invention is a communication apparatus comprising receiving means for receiving data from a first network; storage means for storing the data in a predetermined memory box; transfer means for transferring the data to a destination on a second network; management means for managing destination

information on the second network; and discrimination means for discriminating whether the management means holds an encryption key corresponding to the destination, wherein when the discrimination is affirmative, after encrypting the data by the encryption key, the transfer means is executed, and when the discrimination is negative, the storage means is executed to the data.

[0014]

Preferably, when the discrimination by the discrimination means is negative, a message indicating that the data are stored in the memory box is transmitted to the destination.

[0015]

Preferably, the encryption key is a public key acquired from the destination.

[0016]

Preferably, the invention further comprises secrecy level discrimination means for discriminating the secrecy level of the data, wherein any data a secrecy level of which is low are transferred to the destination without encrypting regardless of the result of the discrimination means.

[0017]

Preferably, the secrecy level discrimination means discriminates whether the data are confidential data.

[0018]

Preferably, the invention further comprises security discrimination means for discriminating security of the transfer path to the destination, wherein when the destination is judged secure, the data is transferred without encrypting regardless of the result of the discrimination means.

[0019]

Preferably, the invention further comprises detection means for detecting that the discrimination of the discrimination means becomes affirmative after executing the storage means, wherein when the detection means detects the affirmative discrimination, the transfer means transfers the data in the memory box.

[0020]

It is also preferable in these inventions that the first network is the public network and the second network is LAN.

[0021]

It is also preferable in these inventions that the first network is the circuit switching network and the transfer path of the second network contains the internet.

[0022]

[Embodiment(s)]

Now the present invention will be clarified in detail by preferred embodiments thereof, with reference to the accompanying drawings.

[0023]

Fig. 1 is a block diagram showing the configuration of a communication apparatus of the present invention, wherein shown are a CPU 101 for controlling the entire apparatus, a ROM 102 storing control programs to be executed by the CPU 101, and a RAM 103 constituting a temporary storage area for the data. A part of the RAM is constructed as a non-volatile memory backed up by a battery or the like, and serving to store data to be retained even after the power supply of the apparatus is turned off, such as registration data and management tables required in the present embodiment. Such non-volatile memory may also be replaced by a hard disk.

[0024]

There are also provided an IPO 104 for data input/output with external circuits, an operation panel 105 controlled by the PIO 104, a compression circuit 106 for compressing data, a decompression circuit 107 for decompressing the data, a modulation circuit 108 for converting data into an analog signal of audible range for transmission to a public network 202, a demodulation circuit 109 for demodulating the analog signal, received from the public network 202, into a digital signal, a modem 110 consisting of the modulation circuit 108 and the demodulation circuit 109, an NCU 111 for connecting the present apparatus with

the public network 202, a LAN controller 112 relating to the protocol for transmitting the signal to the LAN, a LAN connection circuit 113 to be used for matching the level of the signal in the present apparatus with that on the NCL, and a CPU bus 114 to be used for the control by the CPU 101.

[0025]

Fig. 2 illustrates a network system to which the communication apparatus 201 of the present invention is connected. Referring to Fig. 2, the communication apparatus 201 is connected to a public network 202 and a LAN 203. On the LAN 203, there are connected a server computer 205 to be used for example for storing the received image data, and a client computer 206 capable of information exchange with the server computer 205. The server computer 205 is provided with e-mail server functions such as SMTP server function and POP server function, and is so constructed as to be capable of exchanging e-mail with the communication apparatus 201, the client computer 206 and other unrepresented terminals. The communication apparatus 201 and the client computer 206 are naturally provided with an e-mail client function.

[0026]

The communication apparatus 201 executes facsimile communication with the facsimile device 204 through the public network 202.

[0027]

<First embodiment>

In a configuration where the communication apparatus 201 transmits an image received from the public network to the server computer 205 for storage in a predetermined area, the first embodiment selectively executes the encryption of the image according to whether the received image represents a confidential image.

[0028]

In case the received image represents a confidential image, the image is encrypted by a predetermined method and stored thereby being rendered observable only by a specified user. Thus the received confidential image can be transferred while the confidentiality of the image is retained.

[0029]

In the following there will be explained the function of the communication apparatus 201 of the present embodiment, with reference to a flow chart shown in Fig. 3. The sequence is started after the power supply to the communication apparatus 201 is turned on (step S301) and there is entered a state of awaiting a call reception from the public network 202 (step S302). If a call is made from the facsimile device 204 while the call reception is awaited, the call reaches and is received by the communication

apparatus 201 through the public network 202. When the call is detected by the CPU 101 and the NCU 201, the call is established by the NCU 111.

[0030]

Then there is entered a phase B based on the ITU-T recommendation T.30 for executing a training for exchanging the information on communication ability and investigating the quality of the communication line (hereinafter represented as pre-communication). In the pre-communication (step S303), there are informed information such as the aforementioned sub-address (by SUB signal in ITU-T T.30), a password (by PWD signal in ITU-T TT.30) in case of a confidential image, a confidential box number etc. Such information are temporarily stored in the RAM 103 of the communication apparatus 201.

[0031]

After the pre-communication (step S303), there is executed reception of image data (step S304). The image signal transmitted through the public network 202 is fetched into the communication apparatus 201 through the NCU 111, then returned to the original image data through the demodulation circuit 109 of the modem 110 and by the decompression circuit 107, and stored in a predetermined data format (which may be compressed data) in the RAM 103 by the CPU 101. Such receiving operation is repeated until an end notice arrives from

the transmitting side (step S305).

[0032]

After the reception of the image data, there is discriminated whether the image is a confidential image by reading the information stored in the aforementioned RAM 103 (step S306). This discrimination may be made by whether the aforementioned PWD signal is received, or by whether the use of the confidential function is designated on a protocol signal such as the NSS signal.

[0033]

In the case of the communication using the confidential function, the image data stored in the RAM 103 are read by the CPU 101 and the encrypted (step S307). The data are transmitted to the LAN controller 112, and to the LAN 203 through a LAN connection circuit 113, thereby transferring to the server computer 205 (step S308). Also the CPU 101 transmits the password and the confidentiality box number obtained in the pre-communication (step S303) to the server computer 205, whereupon the communication apparatus 201 terminates the sequence (step S409).

[0034]

In the case of the normal communication not using the confidential function at the step S306, the encrypting step S307 is skipped and the image data are transferred without encryption to the server computer 205 (step S308) whereupon the communication apparatus

201 terminates the sequence (step S309).

[0035]

Upon receiving the image data transferred in the step S308, the server computer 205 stores such image data as a file in a memory area thereof and transmits a reception notice of the facsimile data to the client computer 206 of a specified user based on the sub address. Such notice is made for example by e-mail. The user receiving the notice manipulates the client computer 206 for acquiring the image data addressed to the user from the server computer 205 for example by downloading, thereby being enabled to acquire the image data as visible information, for example by display on the client computer 206 with an image viewer application or by printing with an unrepresented printer device.

[0036]

On the other hand, in the case that the facsimile data stored in the server computer 205 are encrypted data, it is necessary to transmit a password corresponding to the confidentiality number to the server computer 205 when the client computer 206 downloads the data from the server computer 205. Only in case the server computer 205 judges that the password is proper, it transmits the decrypted image data to enable displaying thereof on the client computer 206.

[0037]

<Second embodiment>

In a configuration where the communication apparatus 201 transmits an image received from the public network to the server computer 205 for storage in a predetermined area, the second embodiment does not execute such storage but transfers the image data to the designated destination by e-mail in case the received image represents a confidential image.

[0038]

In case the received image data represent a confidential image, the image data are directly e-mail transferred to the destination without storage in the memory of the server computer 205, whereby the received confidential image can be transferred while the confidentiality of the data are retained.

[0039]

In the following there will be explained the function of the communication apparatus 201 of the present embodiment, with reference to a flow chart shown in Fig. 4. As the process of steps S401 to S405 have already been explained in the step S301 to S305 of the foregoing first embodiment, the sequence will be explained in the following from a step S406.

[0040]

At first there is discriminated whether the image data received in the step S405 represents a

confidential image, by reading the information stored in the aforementioned RAM 103 (step S406), and, if a confidential image is represented, the CPU 101 reads the image data stored in the RAM 103 and converts the image data into an image format (JPEG, GIF etc.) developable by the client computer 206 (step S407). Then the CPU 101 specifies the user at the address of transfer by the sub address, and sends an e-mail (step S408) to that user. In this operation, the image data converted to the image format is attached to the e-mail, whereby realized is the delivery of the confidential image to the specified user by e-mail. After the transmission of the e-mail to which attached are the image data converted in to the image format, the communication apparatus 201 terminates the sequence (step S409).

[0041]

In case the step S406 identifies that the received image data do not represent a confidential image, the image data are transferred to the server computer 205 (step S410) whereupon the communication apparatus 201 terminals the sequence (step S409). The server computer 205 stores such image data as a file in a memory area thereof and transmits a reception notice of the facsimile data to the client computer 206 of a specified user based on the sub address (step S411). Such notice is made for example by e-mail. Upon

receiving the notice, the user manipulates the client computer 206 for acquiring the facsimile data addressed to the user from the server computer 205 for example by downloading, thereby being enabled to acquire the image data as visible information, for example by display on the client computer 206 with an image viewer application or by printing with an unrepresented printer device.

[0042]

<Third embodiment>

In transferring the received confidential image by e-mail, the third embodiment selectively executes encryption based on whether a public key of the destination of transfer is acquired.

[0043]

More specifically, in case the communication apparatus 201 has acquired the public key of the destination of transfer of the confidential image, the received image is transferred by an e-mail encrypted with such public key. In case the communication apparatus 201 has not acquired the public key of the destination of transfer of the confidential image, such confidential image is not transferred but is stored in a memory box managed by the communication apparatus 201, and an e-mail only describing that the received confidential image is stored in the memory box is transmitted to the destination of transfer.

[0044]

In the public key system, the encrypting key at the transmitting side is different from the decrypting key at the receiving side, in which one of the keys made public (public key) while the other is maintained secret (secret key). The user, receiving a confidential image encrypted with his public key, can view the confidential image by decryption with the secret key held by the user only.

[0045]

In this manner it is rendered possible to prevent unexpected disclosure of the confidential image without encryption onto the LAN, thereby maintaining the confidentially of the confidential image.

[0046]

Fig. 6 shows a management table held by the communication apparatus 201 and storing the correspondence between the sub address data and the e-mail addresses of the destinations of transfer. The table stores the e-mail addresses of the destinations of data and the memory box numbers for the sub address data 601 in mutual correspondence.

[0047]

Fig. 7 shows, in the form of a table, the data structure of an address notebook in the e-mail client function of the communication apparatus 201. As shown in Fig. 7, for each address, there are shown a

destination name 701, an e-mail address 702 and information 703 whether the public key of such destination is obtained. The public key data are acquired in advance from each destination through the LAN, or from a detachable memory medium by providing the communication apparatus 201 with a function of connecting a device capable of driving such memory medium. The acquired public key data are stored as file data, and the acquired public key data and the destination are correlated in the address notebook through a predetermined procedure.

[0048]

Also in acquiring the public key, it is preferable also to confirm the appropriateness of the public key by receiving a certificate certifying that the public key is of the proper owner from a predetermined certifying organization and then to register the public key in the aforementioned address notebook.

[0049]

In the following the present third embodiment will be explained with reference to Figs. 6 and 7.

[0050]

At first, when the image with designated sub address of "0123" is received from the transmitter, the address of the destination of transfer is converted into "aaa@canon.canon.com" based on the management table shown in Fig. 6, and the presence/absence of the

public key is judged, based on the address of the destination of transfer in the address notebook shown in Fig. 7.

[0051]

In the example shown in Figs. 6 and 7, the confidential images designated for the sub addresses "0123" and "8901" are respectively stored in the corresponding memory boxes "01" and "03" since the public keys are not acquired, and e-mails describing the storing box number, the transmitter information and the time and date of reception as text data are transferred to the respective destinations "aaa@canon.canon.com" and "ccc@canon.canon.com".

[0052]

The confidential image designated for the sub address "4567", for which the public key has been acquired, is encrypted with such public key and is transferred to the destination "bbb@canon.canon.com".

[0053]

Also in case the received image does not represent a confidential image, the received image is transferred by e-mail, without encryption, to the e-mail address of the destination corresponding to the sub address.

[0054]

Fig. 5 is a flow chart showing the function of the communication apparatus 201 in the present third embodiment. As the process of steps S501 to S505 have

already been explained in the step S301 to S305 of the foregoing first embodiment, the sequence will be explained in the following from a step S506.

[0055]

At first a step S506 discriminates whether the image received in the step S504 represents a confidential image, and, if not, the sequence proceeds to a step S512 for transmitting an e-mail with the received image as an attachment to the e-mail address corresponding to the sub address received in the step S503.

[0056]

A step S507 discriminates, based on the management table shown in Fig. 6 and the address notebook shown in Fig. 7, whether the public key is correlated with the e-mail address corresponding to the sub address received in the step S503. If the public key is not correlated, the sequence proceeds to a step S510 for storing the received image in a memory box corresponding to the sub address. Then a step S511 transmits, to the e-mail address corresponding to the sub address, an e-mail describing, as text data, a message that the confidential image is stored in the memory box. An example of the message is "A confidential image is received in your memory box. Please come to receive it".

[0057]

The receiver of the confidential image, receiving the above-mentioned message, visits the location of the communication apparatus 201 and enters a password corresponding to the memory box from the operation panel 10, whereby the confidential image is outputted from the unrepresented printer. In this manner it is rendered possible to prevent unexpected disclosure of the confidential image without encryption onto the LAN, thereby maintaining the confidentiality of the confidential image.

[0058]

In case the step S507 identifies that the public key is correlated, the sequence proceeds to a step S508 for encrypting the received image with such public key, and then a step S509 transfers an e-mail with the confidential image encrypted in the step S509. An example of the encrypting method based on the public key is RSA (Rvert-Shamir-Adleman) system.

[0059]

The above-described process allows secure encryption in transferring the confidential image received from the public circuit through a LAN thereby enabling to maintain the confidentiality of the confidential image.

[0060]

Among the encryption systems, there is also known a common key system, in addition to the aforementioned

public key system. In such common key system, the encrypting key at the transmitting side is same as the decrypting key at the receiving side. The transmitting side executes transmission by encrypting the communication text (plaintext) by such encrypting key, and the receiving side decrypts the received text (encrypted text) with the same key.

[0061]

As the public key system generally requires a longer time in comparison with the common key system, because the encryption and the decryption are more complex, it is also possible to transfer data obtained by encrypting the confidential image by a common key generated by a predetermined algorithm and data obtained by encrypting such common key by the public key of the destination of transfer. An encryption system based on the common key is DES (data encryption standard) system.

[0062]

<Fourth embodiment>

In the foregoing third embodiment, the receiver of the confidential image stored in the memory box in the step S510 is assumed to visit the communication apparatus 201 for obtaining the printed output. In the present fourth embodiment, after the confidential image is stored in the memory box, in response to the registration of the public key of the destination of

transfer of the confidential image in the aforementioned address notebook, such confidential image is automatically encrypted with such public key and transferred to the destination.

[0063]

Consequently the receiver of the confidential image, without visiting the location of the communication apparatus 201, can acquire the confidential image stored in the memory box, by causing the system manager to register the public key or by sending the public key to the communication apparatus 201 through the LAN 203.

[0064]

In the following the function of the communication apparatus 201 in the present fourth embodiment will be explained with reference to a flow chart shown in Fig. 10, which is a modification of the flow chart of the third embodiment and in which any step of a number same as in the third embodiment has a same content. In the following there will only be explained steps of which processes are different from the third embodiment.

[0065]

At first, after the process of the step S512 in Fig. 11, there is executed, at a predetermined interval, a process of discriminating whether the public key of the destination corresponding to the confidential image stored in the memory box is registered in the address

notebook (a loop process consisting of steps S1001 and S1002), and if the step S1001 detects the affirmative discrimination in such loop process, the sequence proceeds to a step S508 for transferring the confidential image with encryption by the registered public key.

[0066]

Also the message to be transmitted in the step S511 can be, for example, "A confidential image is received in your memory box. The confidential image will be encrypted and transmitted if you sends your public key".

[0067]

<Fifth embodiment>

The foregoing third embodiment does not execute the image transfer unless the public key of the destination is acquired, but, in the present embodiment, the encrypted transfer is executed depending on the security of the transfer path. More specifically, in the transfer through the LAN 203, there is discriminated whether the public key of the destination of transfer is acquired or not only in case the security of the transfer path is not ensured, and, if the public key is discriminated to be present, the confidential image is encrypted and transferred, but, if absent, the confidential image is stored in the memory box and a message indicating such image storage

alone is transmitted to the destination. Also in case the security of the transfer path is ensured, the confidential image is transferred to the destination regardless whether the public key of the destination of transfer is acquired or not.

[0068]

In this manner the process relating to the public key data can be dispersed with for the destinations within a domain with ensured security such as an intranet, whereby the process of registered data management in the communication apparatus 201 can be alleviated.

[0069]

In the following the function of the communication apparatus 201 in the present fifth embodiment will be explained with reference to a flow chart shown in Fig. 11, which is a modification of the flow chart of the third embodiment, and in which any step of a number same as in the third embodiment has the same content. In the following there will only be explained steps of which processes are different from the third embodiment.

[0070]

At first, if the step S506 identifies that the received image data represent a confidential image, the sequence proceeds to a step S1101. A step S1101 judges the security of the transfer path to the destination of transfer corresponding to the sub address received in

the step S503, and, if the transfer path is judged secure, the sequence proceeds to a step S512 for transferring the confidential image to the destination.

[0071]

On the other hand, if the transfer path is judged not secure, the sequence proceeds to a step S507 for determining whether to transfer the confidential image or to store it in the memory box, according to the presence or absence of the public key. The judgment of the security of the transfer path in the step S1101 can be made, for example, by the domain of the e-mail address of the communication apparatus 210 and the domain of the e-mail address of the destination of transfer.

[0072]

Such judgment will be explained in more detail with reference to Figs. 6 and 7. As explained in the foregoing, the communication apparatus 201 is provided with an e-mail client function, for example with an e-mail account "fax@canon.canon.com".

[0073]

Consequently, in the example of the address notebook data shown in Fig. 7, the destinations aaa, bbb and ccc are in the same domain "canon.canon.com" of the communication apparatus 201 while the destinations ddd and eee are in domains different from that of the communication apparatus 201.

[0074]

Therefore, for the destinations of transfer belonging to the domain of the communication apparatus 201, the confidential image is transferred by the e-mail regardless whether the public key is registered in the address notebook.

[0075]

For the destination in a domain different from that of the communication apparatus 201, the transfer is executed according to whether the public key is registered in the address notebook. More specifically, since the public key is not registered for the destination ddd, the confidential image for the destination ddd is stored in the memory box and the e-mail describing only a message indicating the storage of the confidential image in the memory box is transmitted to the destination ddd. Also as the public key is registered for the destination eee, the e-mail with the confidential image encrypted with the public key is transmitted to the destination eee.

[0076]

The domain name has a hierarchic layered structure punctuated by dots, and the judgment of a same domain by the coincidence of a number of hierarchic layers starting from the first layer "com" depends on the security policy of the network system. For example the transfer path may be judged secure by the coincidence

up to the second hierarchic layer "canon.com".

[0077]

In the foregoing there has been explained the judgment based on the domain name, but the security may also be judged by whether the sub net of the IP address of the destination of transfer is within a predetermined sub net.

[0078]

<Sixth embodiment>

The foregoing embodiments have been explained by the function of a single equipment constructed as the communication apparatus, but the present invention may also be applied to a system consisting of plural equipment such as a personal computer, a modem, a scanner, a printer etc. The configuration of such system will be briefly explained with reference to Fig. 8. Referring to Fig. 8, a personal computer (PC) 801 is connected to a scanner 801, a printer 803 and a modem 804 (which may be incorporated in the PC 802) through a predetermined interface. The PC 802 is also connected to a public network 202 through the modem 804 and to a LAN 203 through an unrepresented LAN board.

[0079]

The interface connecting the PC 802 with the scanner 801, printer 803 and modem 804 may be a network interface through the LAN 203, but is preferably a local interface separated from the LAN 203, such as USB,

in order to handle the secret data such as the confidential image.

[0080]

In the following there will be explained the receiving operation in this system. At first, a signal transmitted from the public network 202 is fetched into the modem 805 through a NCU unit incorporated therein. The modem 805 demodulates the analog signal to restore the digital data. The digital data are read by a computer 807 in which image data are restored by decompression of the compressed data and are supplied to a printer 808, which prints the image data.

[0081]

If the received image is confidential, the data are stored in a memory box of a hard disk device incorporated in the PC 802, and, according to the aforementioned third embodiment, the confidential image is transferred with encryption by the public key to the destination of which the public key is acquired while the e-mail indicating the reception of the confidential image is transmitted to the destination of which the public key is not acquired.

[0082]

In the foregoing first to sixth embodiments, there has been explained a configuration in which the sub address received from the transmitting side in converted by the communication apparatus of the present

invention into the e-mail address, but the e-mail address of the destination of transfer may be directly set in the sub address from the transmitting side.

[0083]

Also in the foregoing embodiments, there has been explained a case of transferring the image, received from the public network 202, to the client device on the LAN 203, but such configuration is not restrictive and there may be assumed a configuration in which the LAN 203 is connected to the internet through a predetermined access point and the image data received from the public network 202 is transferred through the internet. The present invention is suitable for the communication through the internet since the security is considered important in such communication.

[0084]

The present invention is also applicable to a case in which the image received from the public network is transferred by dial-up connection to the access point of the internet from the public network.

[0085]

Also the present invention is naturally applicable to a case where the present invention is realized by the supply of a program to a system or an apparatus. In such case, the objects of the present invention can be attained by a computer (PCU or MPU) of such system or apparatus, reading and executing the program codes

stored in a memory medium and realizing the present invention.

[0086]

Also the present invention naturally includes a case where, in executing the read program codes by the computer, an OS (operating system) functioning on the computer executes a part of the processes.

[0087]

[Effect of the Invention]

As explained so far, according to the present invention, a confidential image received from the public network is encrypted and stored in the server computer on a LAN, so that any user other than the specified client cannot easily view the confidential image. This makes it possible to deliver the confidential image to the client on the LAN while the confidentiality is retained.

[0088]

Also, according to the present invention, since a confidential image received is transmitted to a user, who is a receiver of the image, by attaching the image to an e-mail, it becomes unnecessary for the user to go to the communication apparatus and print the confidential image so that the user's operational load can be reduced substantially.

[0089]

According to the present invention, if an

encryption key of the destination is retained, the image is transferred after encrypting by the encryption key and if not, the image is stored in a specified memory box, so that it is rendered possible to prevent unexpected disclosure of the confidential image onto the LAN without encryption.

[0090]

According to the present invention, if it is detected that the encryption key of the destination of the confidential image is registered after the confidential image is stored in the memory box, the confidential image is automatically encrypted by the public key and transferred to the destination, so that there is no need for the user to go to the apparatus to receive the confidential image.

[0091]

According to the present invention, the image is encrypted and transferred based on security of the transfer path, so that for the transfer within the network whose security is assured, there is no need to exchange the encryption key, thereby reducing the burden of an apparatus administrator.

[Brief Description of the Drawings]

[Fig. 1] A view showing the configuration of a communication apparatus constituting a first embodiment of the present invention.

[Fig. 2] A view showing a network system in the

first embodiment of the present invention.

[Fig. 3] A flow chart showing the function of the communication apparatus of the first embodiment of the present invention.

[Fig. 4] A flow chart showing the function of the communication apparatus in a second embodiment of the present invention.

[Fig. 5] A flow chart showing the function of the communication apparatus in a third embodiment of the present invention.

[Fig. 6] A view showing the data structure of a management table indicating the correspondence between sub addresses and electronic mail addresses in the third embodiment of the present invention.

[Fig. 7] A view showing the data structure of an address notebook in the third embodiment of the present invention.

[Fig. 8] A view showing the configuration of a communication system in a sixth embodiment of the present invention.

[Fig. 9] A view illustrating the prior art.

[Fig. 10] A flow chart showing the function of the communication apparatus in a fourth embodiment of the present invention.

[Fig. 11] A flow chart showing the function of the communication apparatus in a fifth embodiment of the present invention.

[Description of Reference Numerals or Symbols]

101 CPU
102 ROM
103 RAM
104 PIO
105 Operation panel
106 Compression circuit
107 Decompression circuit
108 Modulation circuit
109 Demodulation circuit
110 Modem
111 NCU
112 LAN controller
113 LAN connection circuit
114 CPU bus
201 Communication apparatus
202 Public network
203 LAN
204 Facsimile device
205 Server computer
206 Client computer

[Name of the Document] Abstract

[Abstract]

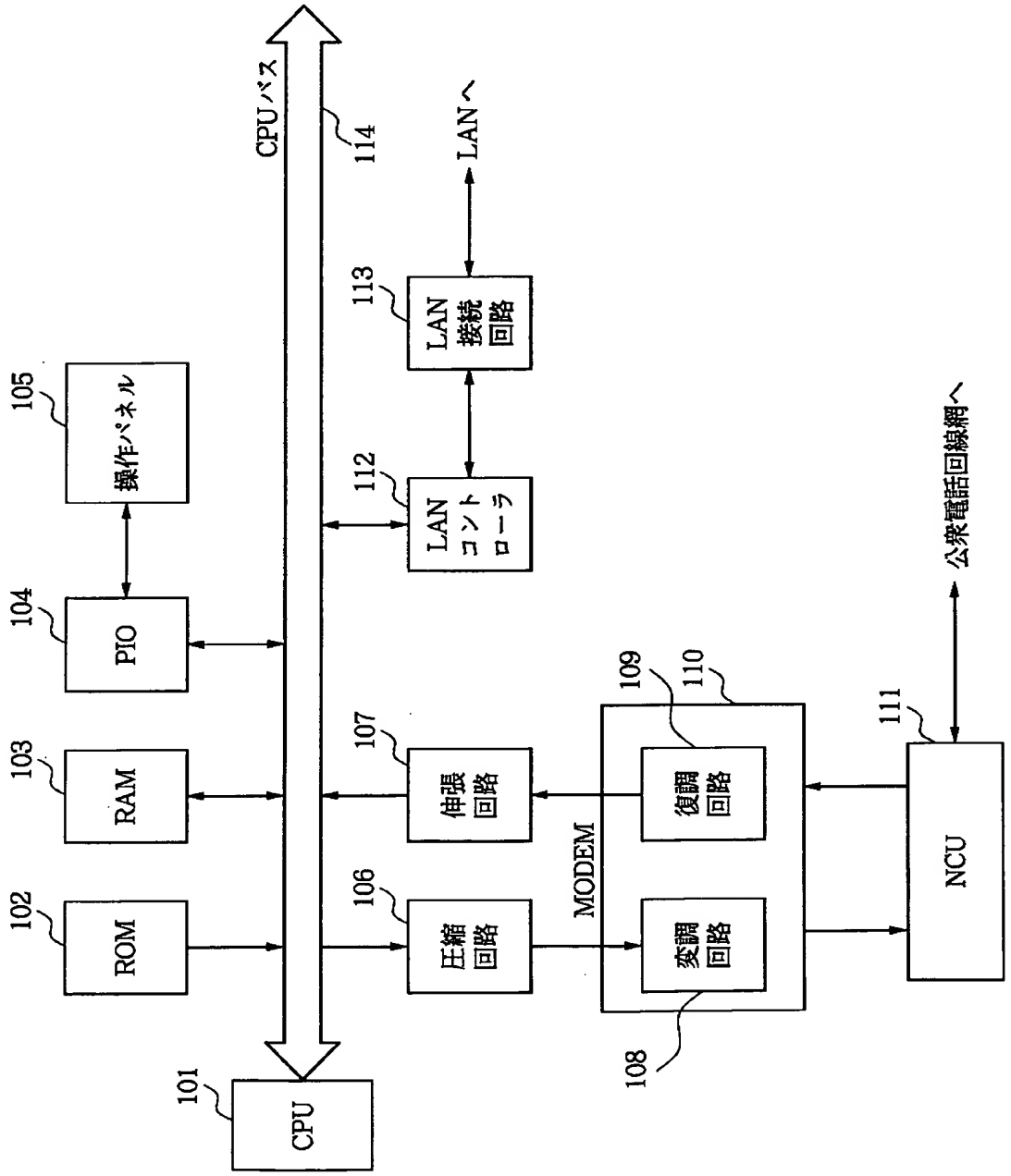
[Problem(s)] An object of the present invention is to provide a communication apparatus capable of transferring the received confidential image to a predetermined destination while maintaining its confidential character, and a method and a memory medium therefor.

[Means for Solving the Problem(s)] At step S306, if the received image is confidential, after the image data are encrypted (step S307), the data are transferred to the server computer onto the LAN (step S308). If the received image is not confidential, the encrypting step S307 is skipped and the image data are transferred without encryption to the server computer 205 (step S308) whereupon the communication apparatus 201 terminates the sequence (step S309).

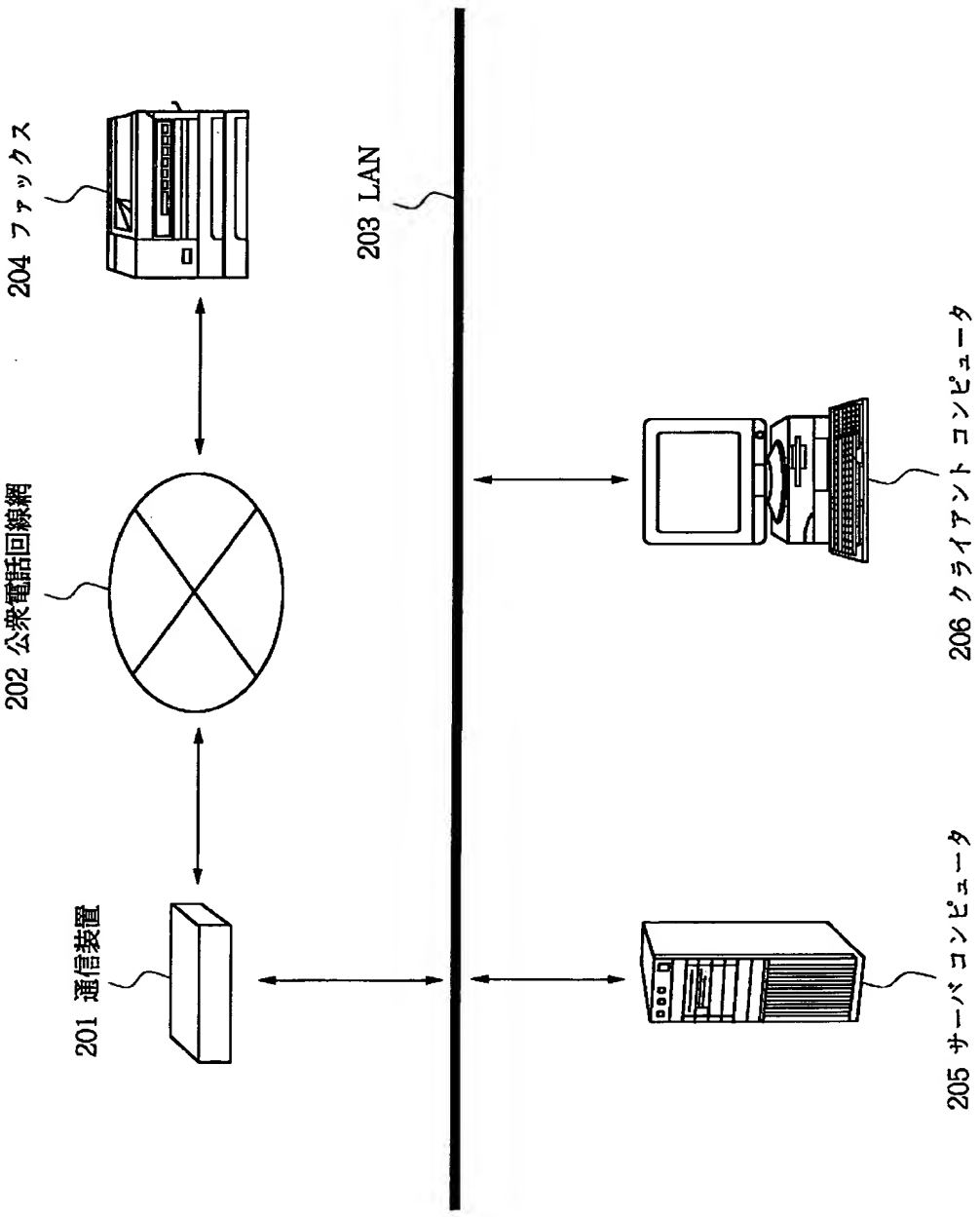
[Elected Drawing] Fig. 3

【書類名】　　図面

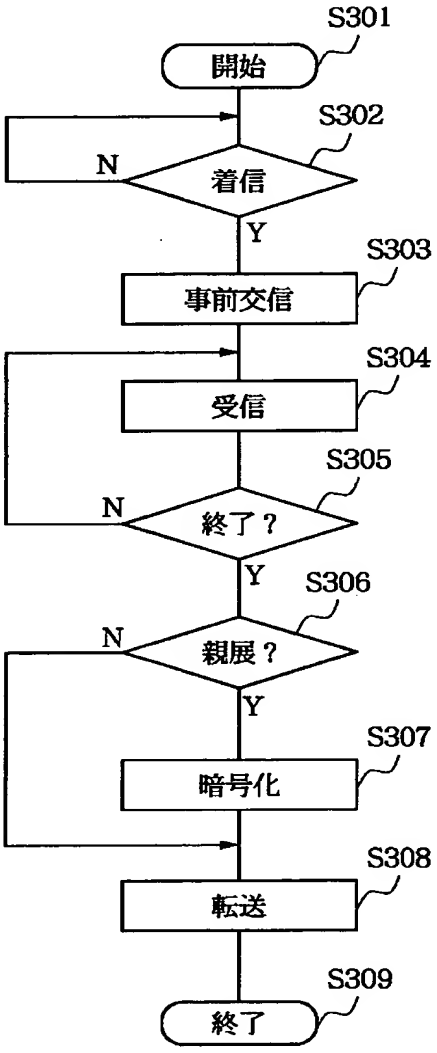
【図１】



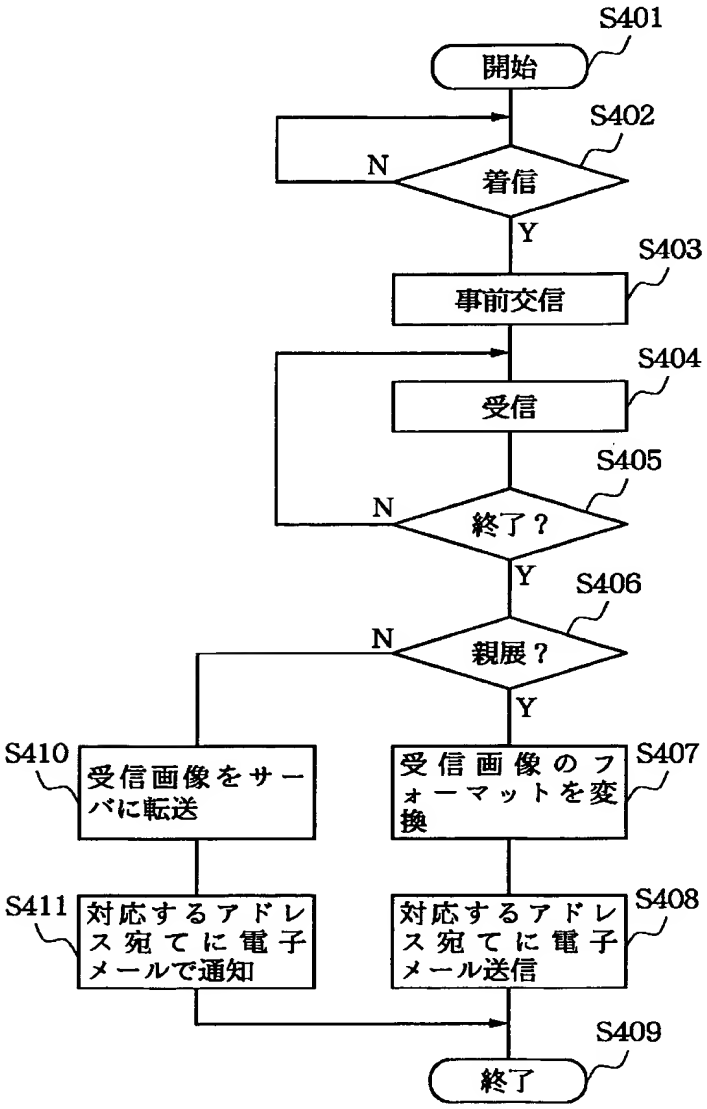
【図２】


204 ファックス
203 LAN
202 公衆電話回線網
206 クライアント コンピュータ
201 通信装置
205 サーバ コンピュータ

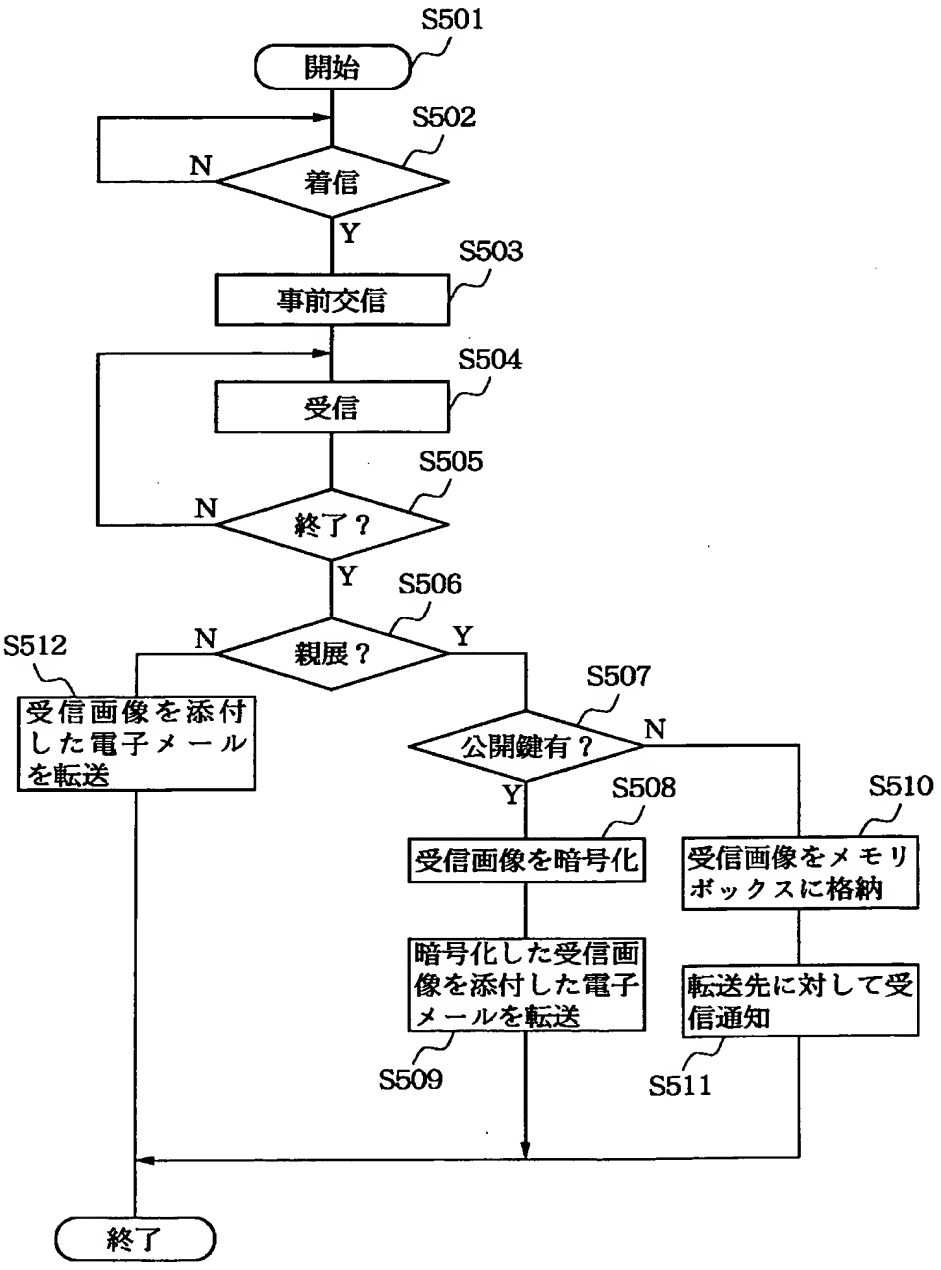
【図３】


S301
開始
S302
着信
N
Y
S303
事前交信
S304
受信
S305
終了？
N
Y
S306
親展？
N
Y
S307
暗号化
S308
転送
S309
終了

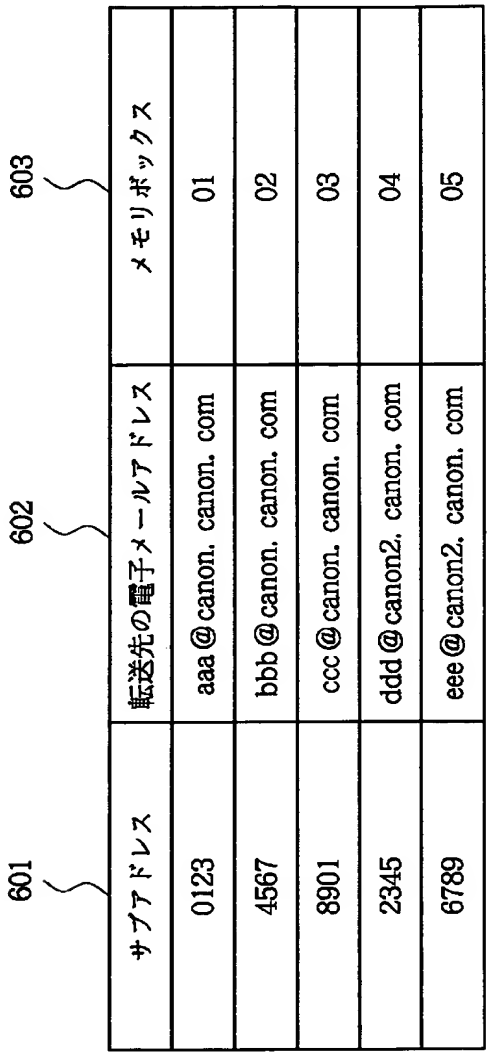
【図４】


S401
開始
S402
着信
N
Y
S403
事前交信
S404
受信
S405
終了？
N
Y
S406
親展？
N
Y
S410
受信画像をサーバに転送
S407
受信画像のフォーマットを変換
S411
対応するアドレス宛てに電子メールで通知
S408
対応するアドレス宛てに電子メール送信
S409
終了

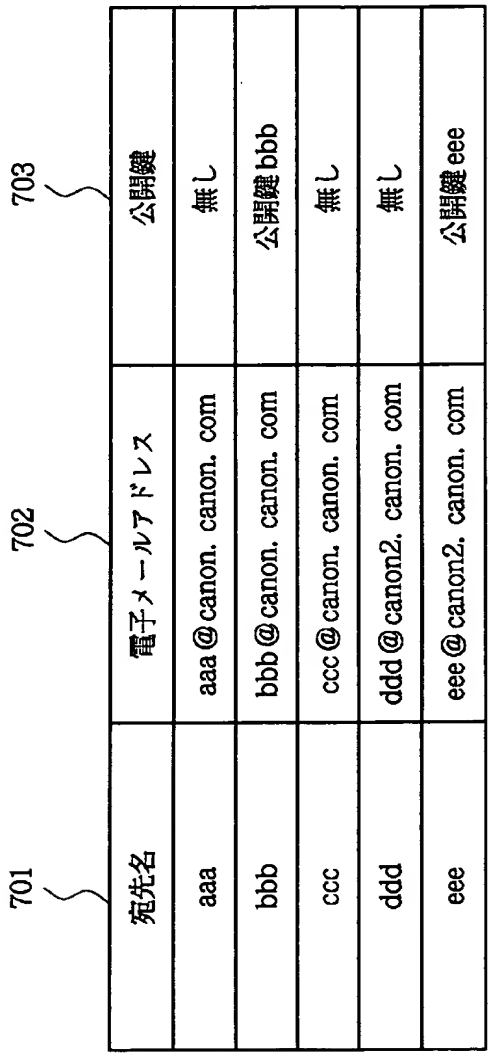
【図５】


S501
開始
S502
着信
N
Y
S503
事前交信
S504
受信
S505
終了？
N
Y
S506
親展？
N
Y
S512
受信画像を添付した電子メールを転送
S507
公開鍵有？
N
Y
S508
受信画像を暗号化
S510
受信画像をメモリボックスに格納
暗号化した受信画像を添付した電子メールを転送
S509
転送先に対して受信通知
S511
終了

【図６】

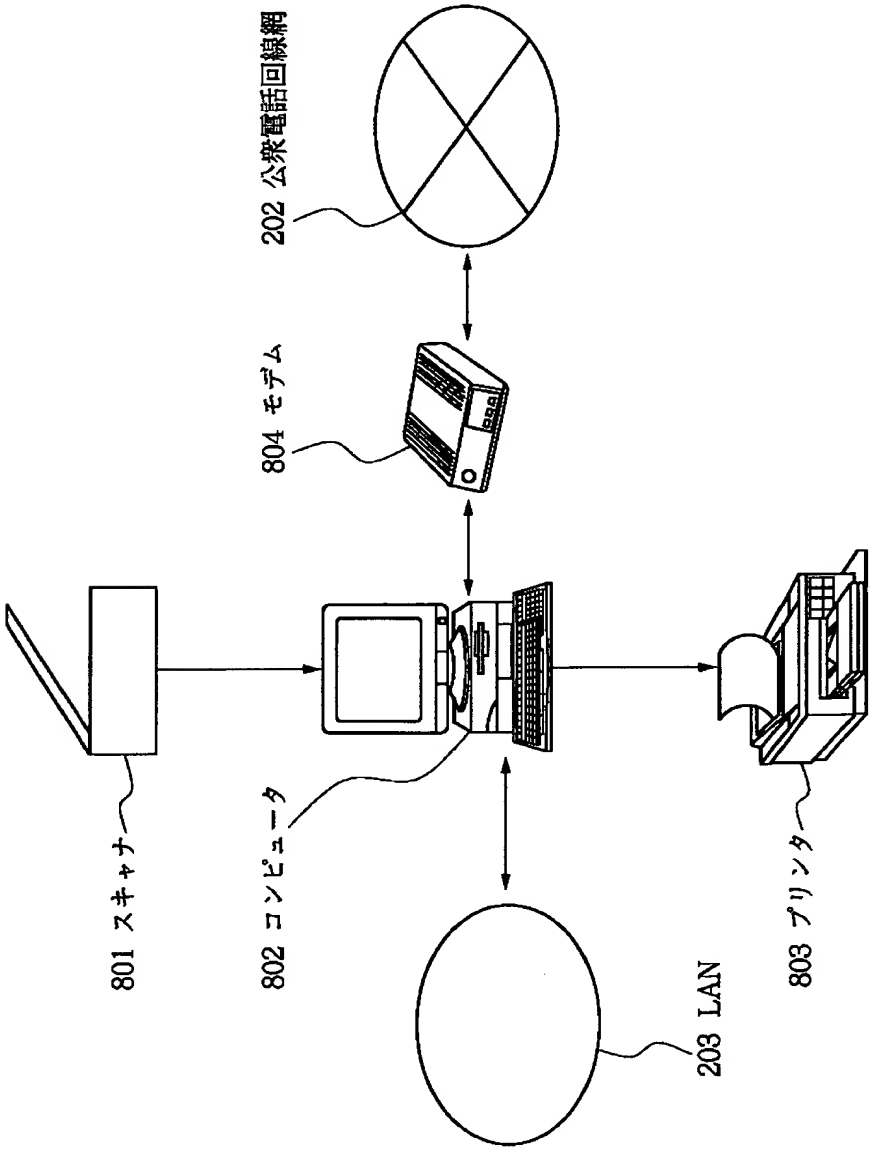

601
602
603
サブアドレス
転送先の電子メールアドレス
メモリボックス
0123
aaa@canon.canon.com
01
4567
bbb@canon.canon.com
02
8901
ccc@canon.canon.com
03
2345
ddd@canon2.canon.com
04
6789
eee@canon2.canon.com
05

【図７】

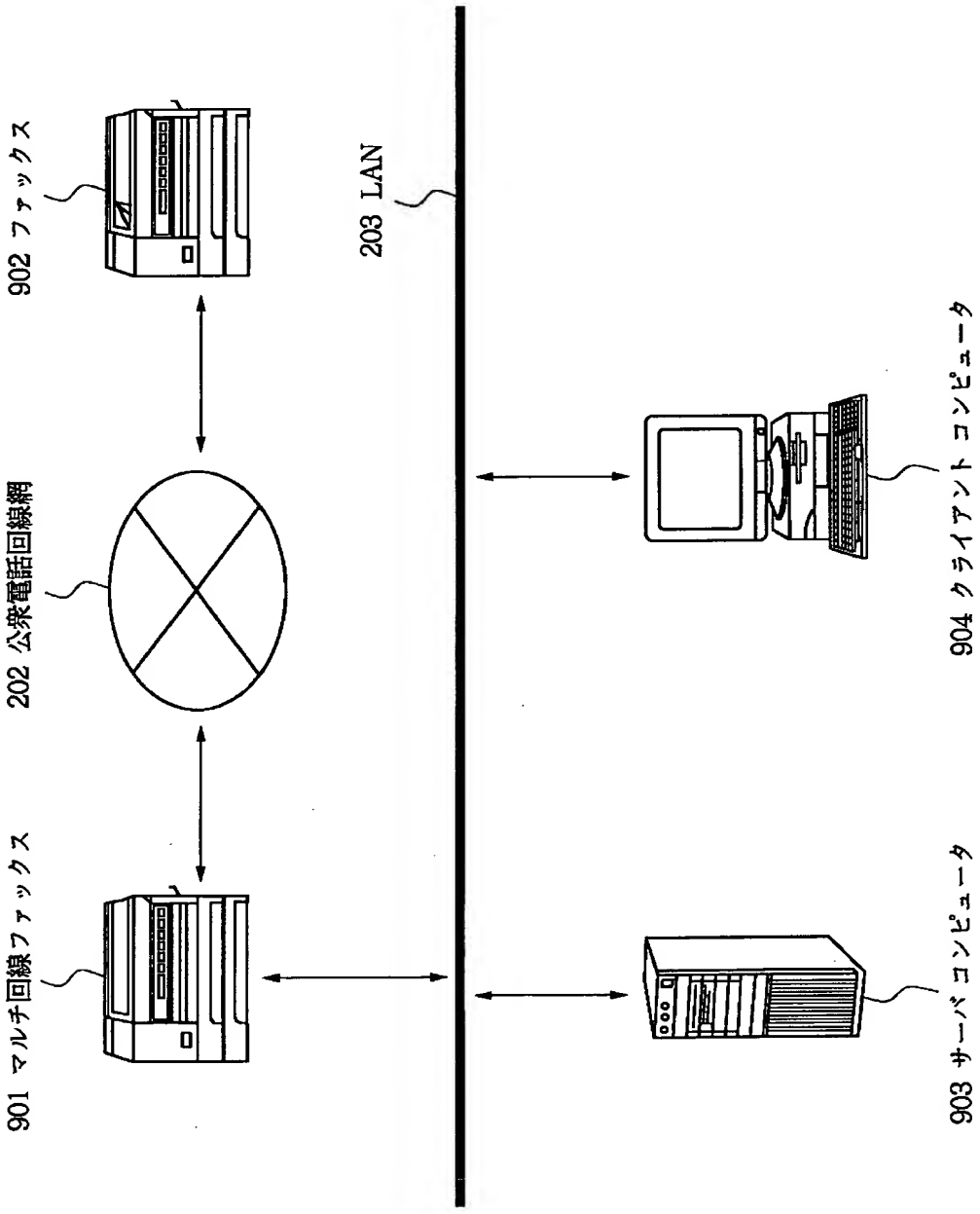


701 宛先名	702 電子メールアドレス	703 公開鍵
aaa	aaa@canon.canon.com	無し
bbb	bbb@canon.canon.com	公開鍵bbb
ccc	ccc@canon.canon.com	無し
ddd	ddd@canon2.canon.com	無し
eee	eee@canon2.canon.com	公開鍵eee

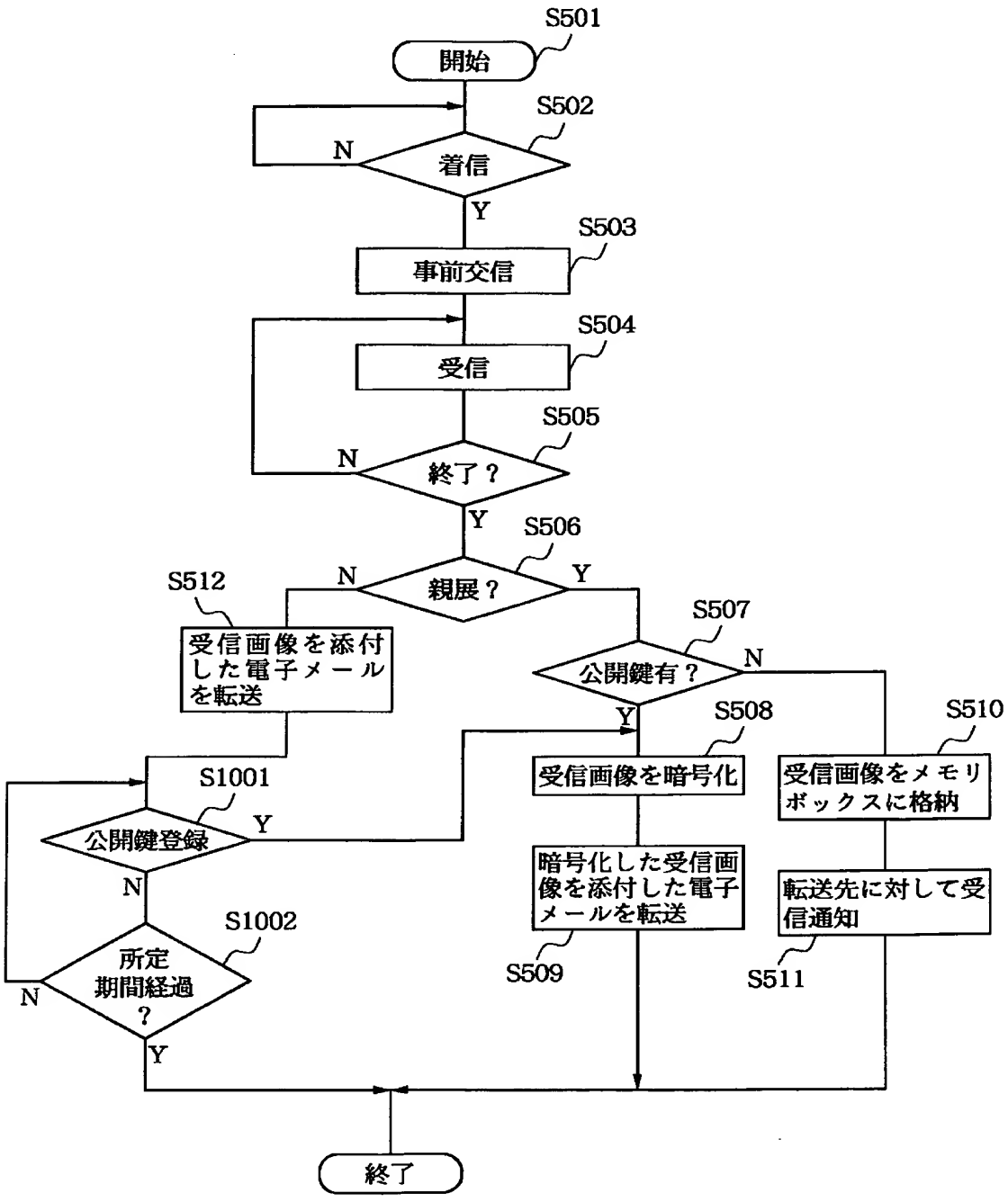
【図８】



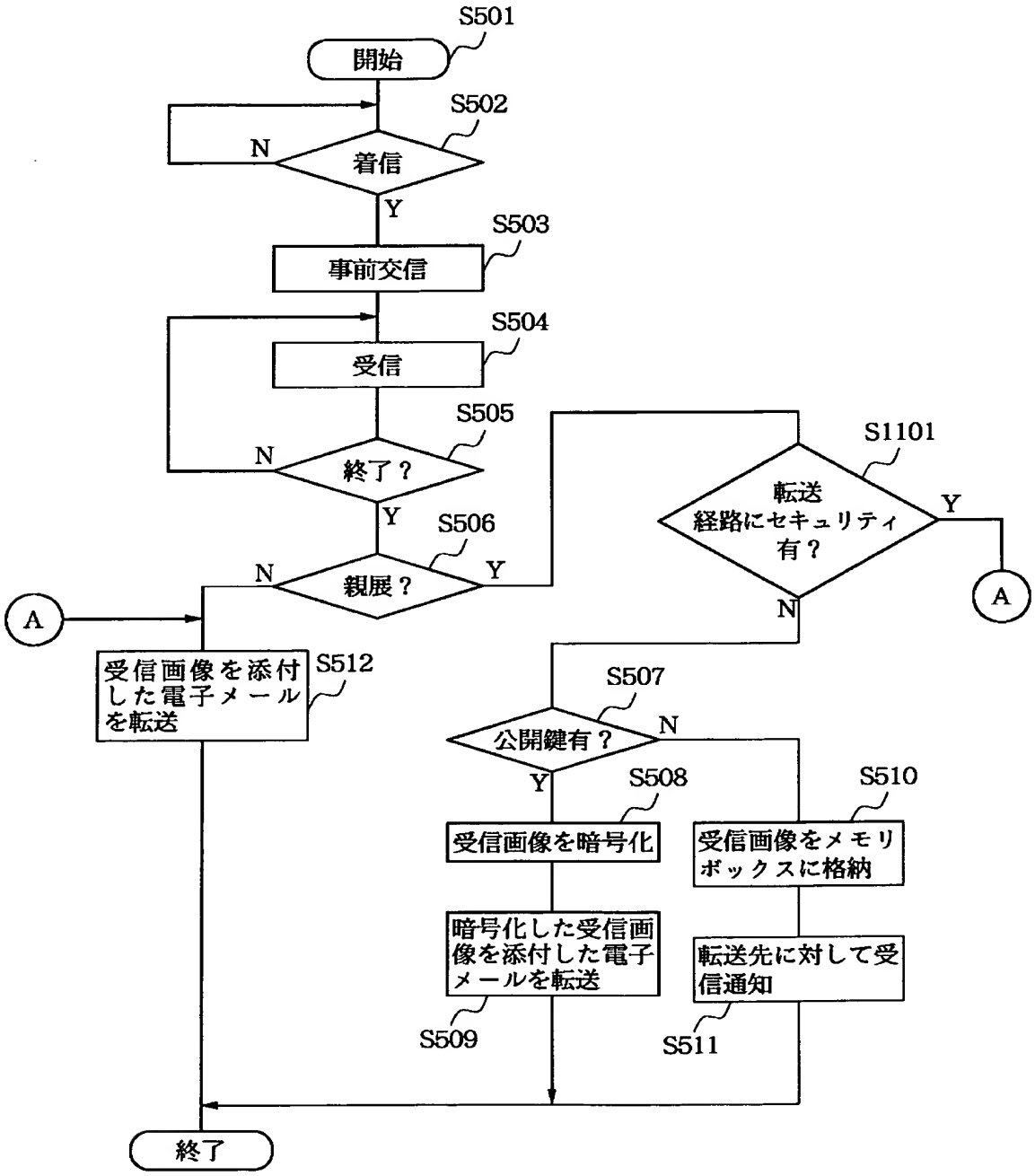
【図９】


902 ファックス
203 LAN
202 公衆電話回線網
904 クライアントコンピュータ
901 マルチ回線ファックス
903 サーバコンピュータ

【図１０】


S501
開始
S502
着信
N
Y
S503
事前交信
S504
受信
S505
終了？
N
Y
S506
親展？
N
Y
S512
受信画像を添付した電子メールを転送
S507
公開鍵有？
N
Y
S508
受信画像を暗号化
S510
受信画像をメモリボックスに格納
S1001
公開鍵登録
Y
N
暗号化した受信画像を添付した電子メールを転送
S509
転送先に対して受信通知
S511
S1002
所定期間経過？
N
Y
終了

【図１１】


S501
開始
S502
着信
N
Y
S503
事前交信
S504
受信
S505
終了？
N
Y
S506
親展？
N
Y
A
受信画像を添付した電子メールを転送
S512
S1101
転送経路にセキュリティ有？
Y
N
A
S507
公開鍵有？
N
Y
S508
受信画像を暗号化
暗号化した受信画像を添付した電子メールを転送
S509
S510
受信画像をメモリボックスに格納
転送先に対して受信通知
S511
終了

[Name of the Document] Drawings

Fig. 1

105 Operation panel

106 Compression circuit

107 Decompression circuit

108 Modulation circuit

109 Demodulation circuit

112 LAN controller

113 LAN connection circuit

114 CPU bus

LANへ To LAN

公衆電話回線網へ To public telephone network

Fig. 2

201 Communication apparatus

202 Public telephone network

204 Facsimile device

205 Server computer

206 Client computer

Fig. 3

S301 Start

S302 Incoming call?

S303 Pre-communication

S304 Reception

S305 End?

S306 Confidential?

S307 Encryption

S308 Transfer

S309 End

Fig. 4

S401 Start

S402 Incoming call?

S403 Pre-communication

S404 Reception

S405 End?

S406 Confidential?

S407 Convert received image format

S408 Transmit e-mail to corresponding address

S410 Transfer received image to server

S411 Notify to corresponding address by e-mail

S409 End

Fig. 5

S501 Start

S502 Incoming call?

S503 Pre-communication

S504 Reception

S505 End?

S506 Confidential?

S507 Public key exists?

S508 Encrypt received image

S509 Transfer e-mail attached with encrypted received image

S510 Store received image into memory box

S511 Notify reception to transfer destination

S512 Transfer e-mail attached with received image

終了 End

Fig. 6

601 Sub address

602 e-mail address of destination

603 Memory box

Fig. 7

701 Destination name

702 e-mail address

703 Public key

無し None

公開鍵 Public key

Fig. 8

202 Public telephone network

801 Scanner

802 Computer

803 Printer

804 Modem

Fig. 9

901 Multi-line facsimile device

202 Public telephone network

902 Facsimile device

903 Server computer

904 Client computer

Fig. 10

S501 Start

S502 Incoming call?

S503 Pre-communication

S504 Reception

S505 End?

S506 Confidential?

S507 Public key exists?

S508 Encrypt received image

S509 Transfer e-mail attached with encrypted received image

S510 Store received image into memory box

S511 Notify reception to transfer destination

S512 Transfer e-mail attached with received image

S1001 Register public key?

S102 Predetermined time interval elapsed?

終了 End

Fig. 11

S501 Start

S502 Incoming call?

S503 Pre-communication

S504 Reception

S505 End?

S506 Confidential?

S507 Public key exists?

S508 Encrypt received image

S509 Transfer e-mail attached with encrypted received image

S510 Store received image into memory box

S511 Notify reception to transfer destination

S512 Transfer e-mail with received image

S1101 Security exists on transfer path?

終了 End

【書類名】　　要約書

【要約】

【課題】　受信した親展画像を、その機密性を維持したまま所定の宛先に転送することが可能な通信装置及び方法並びに記憶媒体を提供することを目的とする。

【解決手段】　ステップＳ３０６において、受信画像が親展の場合は、該画像データの暗号化処理を行った（ステップＳ３０７）後、ＬＡＮ上のサーバコンピュータへと転送する（ステップＳ３０８）。受信画像が親展でない場合は、暗号化の処理であるステップＳ３０７はパスされ、画像データを暗号化せずにサーバコンピュータ２０５へと転送（ステップＳ３０８）し、通信装置２０１は処理を終了する（ステップＳ３０９）。

また、転送先の公開鍵の有無に基づいて、受信した親展画像を転送するか、または、メモリボックス内に格納して転送先に受信通知のみを行うかを決定する。

【選択図】　　図３